Mathematical Journal of Okayama University

Volume 34, *Issue* 1 1992 *Article* 4

JANUARY 1992

On H-separable Polynomials in Skew Polynomial Rings of Automorphism Type

Shoichi Ikehata* George Szeto†

*Okayama University
†Bradley University

Math. J. Okayama Univ. 34 (1992), 49—55

ON H-SEPARABLE POLYNOMIALS IN SKEW POLYNOMIAL RINGS OF AUTOMORPHISM TYPE

Dedicated to Professor Manabu Harada on his 60th birthday

SHŌICHI IKEHATA and GEORGE SZETO

In [2], [3] and [4], one of the authors has studied H-separable polynomials in skew polynomial rings. In [4], we have studied H-separable polynomials of prime degree in skew polynomial rings of automorphism type. The present paper is a natural continuation of [4].

Throughout this paper, B will represent a ring with 1, and ρ an automorphism of B. Let $B[X;\rho]$ be the skew polynomial ring in which the multiplication is given by $bX = X\rho(b)$ $(b \in B)$. A ring extension S/B is called a separable extension if the S-S-homomorphism of $S \otimes_B S$ onto S defined by $a \otimes b \mapsto ab$ splits, and S/B is called an H-separable extension if $S \otimes_B S$ is S-S-isomorphic to a direct summand of a finite direct sum of copies of S. A monic polynomial f in $B[X;\rho]$ with $fB[X;\rho] = B[X;\rho]f$ is called a separable (resp. H-separable) polynomial if $B[X;\rho]/fB[X;\rho]$ is a separable (resp. H-separable) extension of B. It is well known that every H-separable extension is a separable extension. As to terminologies used in this note, we follow [2].

In [4, Theorem 2], for any prime number p, we have shown that the center Z of B is a Galois extension over Z^ρ with the Galois group $(\rho|Z)$ whose order is p if and only if $B[X;\rho]$ contains an H-separable polynomial of degree p. In this paper, for general m, we shall characterize the condition that Z is a Galois extension over Z^ρ with the Galois group $(\rho|Z)$ whose order is m in terms of H-separable extensions (Theorem 1). Moreover, we shall obtain a sharpening of [4, Theorem 4]. Some more results will be obtained in [5].

We shall use the following conventions:

Z = the center of B.

$V_S(B)$ = the centralizer of B in S for a ring extension S/B.

$B^\rho = \{\alpha \in B \mid \rho(\alpha) = \alpha\}$, $Z^\rho = \{\alpha \in Z \mid \rho(\alpha) = \alpha\}$.

Let f be a monic polynomial in $B[X;\rho]$ with $fB[X;\rho] = B[X;\rho]f$. Then we shall denote $B[x;\rho] = B[X;\rho]/fB[X;\rho]$, where $x = X + B[X;\rho]/fB[X;\rho]$, and $B[x^i;\rho^i]$ = the subring of $B[x;\rho]$ generated by B and x^i.

Recall that if f is an H-separable polynomial in $B[X;\rho]$ of degree m, then $f = X^m - u$, u is invertible in B^ρ and $\alpha u = u\rho^m(\alpha)$ $(\alpha \in B)$ ([3, Lemma 1]).

First, we shall state the following theorem which is a generalization of [4, Theorem 2].

Theorem 1. *Let $f = X^m - u$ be in $B[X;\rho]$ with $fB[X;\rho] = B[X;\rho]f$. Then the following are equivalent :*

(a) *u is invertible in B^ρ, and Z/Z^ρ is a G-Galois extension, where G is the group generated by $\rho|Z$ of order m.*

(b) *$B[x^n;\rho^n]$ is an H-separable extension over B for every divisor n of m.*

Proof. (a) $\Longrightarrow$ (b). Assume $m = nd$. Then we have

$$B[x^n;\rho^n] \cong B[Y;\rho^n]/(Y^d - u)B[Y;\rho^n],$$

where $\alpha Y = Y\rho^n(\alpha)$ ($\alpha \in B$), and it is clear that $(Y^d - u)B[Y;\rho] = B[Y;\rho](Y^d - u)$. Since Z/Z^ρ is a G-Galois extension, Z/Z^{ρ^n} is $(\rho^n|Z)$-Galois extension and $(\rho^n|Z)$ is of order d. Hence, by [2, Proposition 1.4] $Y^d - u$ is an H-separable polynomial in $B[Y;\rho^n]$, and so $B[x^n;\rho^n]$ is an H-separable extension B.

To prove the converse, we need the following elementary lemma:

Lemma 2. *If there exist divisors $n_1, n_2, \cdots, n_r$ of m such that $m = n_1 n_2 \cdots n_r$ and in the tower*

$$Z = Z^{\rho^m} \supset \cdots \supset Z^{\rho^{n_i n_{i+1}\cdots n_r}} \supset Z^{\rho^{n_{i+1}n_{i+2}\cdots n_r}} \supset \cdots \supset Z^{\rho^{n_r}} \supset Z^\rho,$$

each $Z^{\rho^{n_i n_{i+1}\cdots n_r}}/Z^{\rho^{n_{i+1}n_{i+2}\cdots n_r}}$ is a $(\rho^{n_{i+1}n_{i+2}\cdots n_r}|Z^{\rho^{n_i n_{i+1}\cdots n_r}})$-Galois extension, where the group $(\rho^{n_{i+1}n_{i+2}\cdots n_r}|Z^{\rho^{n_i n_{i+1}\cdots n_r}})$ is of order n_i $(1 \le i \le r)$, then Z/Z^ρ is a $(\rho|Z)$-Galois extension, where the group $(\rho|Z)$ is of order m.

Proof. By [1, Theorem 1.3], there exist elements $\alpha_k^{(i)}, \beta_k^{(i)} \in Z^{\rho^{n_i n_{i+1}\cdots n_r}}$ such that

$$\sum_k \alpha_k^{(i)} \rho^{\nu n_{i+1}n_{i+2}\cdots n_r}(\beta_k^{(i)}) = \delta_{0,\nu} \quad (0 \le \nu \le n_i - 1, 1 \le i \le r).$$

Then we can easily verify that

$$\sum_{k_1,k_2,\cdots,k_r} \alpha_{k_1}^{(1)}\alpha_{k_2}^{(2)} \cdots \alpha_{k_r}^{(r)} \rho^\nu(\beta_{k_r}^{(r)}\beta_{k_{r-1}}^{(r-1)} \cdots \beta_{k_1}^{(1)}) = \delta_{0,\nu} \quad (0 \le \nu \le m-1).$$

Therefore we have the assertion by [1, Theorem 1.3] again.

Now, we come back to prove Theorem 1. (b) $\Longrightarrow$ (a).

Assume $m = p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k}$, where each p_i are different prime numbers and $e_i > 0$. We define the sequence $n_1, n_2, \cdots, n_r$ of divisors of m as follows:

$$n_i = \begin{cases} p_1 & (1 \leq i \leq e_1) \\ p_2 & (1+e_1 \leq i \leq e_1+e_2) \\ \cdots\cdots\cdots & \\ p_k & (1+e_1+e_2+ \cdots e_{k-1} \leq i \leq e_1+e_2+ \cdots +e_k), \end{cases}$$
$$r = e_1+e_2+ \cdots e_k \quad \text{and} \quad 1 \leq i \leq r.$$

Then $m = n_1 n_2 \cdots n_r$. We shall prove that in the tower

$$Z = Z^{\rho^m} \supset \cdots \supset Z^{\rho^{n_i n_{i+1} \cdots n_r}} \supset Z^{\rho^{n_{i+1} n_{i+2} \cdots n_r}} \supset \cdots \supset Z^{\rho^{n_r}} \supset Z^{\rho},$$

each $Z^{\rho^{n_i n_{i+1} \cdots n_r}} / Z^{\rho^{n_{i+1} n_{i+2} \cdots n_r}}$ is a $(\rho^{n_{i+1} n_{i+2} \cdots n_r} | Z^{\rho^{n_i n_{i+1} \cdots n_r}})$-Galois extension of order n_i $(1 \leq i \leq r)$.

We put here $s = n_{i+1} n_{i+2} \cdots n_r$ and $t = n_i n_{i+1} \cdots n_r$. Then $t = s n_i$, and we may assume

$$t = p_j^{\nu_j+1} p_{j+1}^{e_{j+1}} \cdots p_k^{e_k} \quad \text{and} \quad s = p_j^{\nu_j} p_{j+1}^{e_{j+1}} \cdots p_k^{e_k}, \quad \text{so } t = s p_j.$$

Now we have

$$B[x^s ; \rho^s] \supset B[x^t ; \rho^t] = B[x^{sp_j} ; \rho^{sp_j}] \supset B.$$

Since $B[x^t ; \rho^t] \cong B[Y ; \rho^t]/(Y^q - u)B[Y ; \rho^t]$, where $m = qt$, $Y^q - u$ is an H-separable polynomial in $B[Y ; \rho^t]$. Naturally, we can extend ρ^s to the automorphism $\tilde{\rho}^s$ of $B[x^{sp_j} ; \rho^{sp_j}]$. Consider the skew polynomial ring $B[x^{sp_j} ; \rho^{sp_j}][T ; \tilde{\rho}^s]$, where $\alpha T = T \tilde{\rho}^s(\alpha)$ $(\alpha \in B[x^{sp_j} ; \rho^{sp_j}])$. Then we have the following $B[x^{sp_j} ; \rho^{sp_j}]$-ring isomorphism

$$B[x^s ; \rho^s] \cong B[x^{sp_j} ; \rho^{sp_j}][T ; \tilde{\rho}^s]/(T^{p_j} - x^{sp_j})B[x^{sp_j} ; \rho^{sp_j}][T ; \tilde{\rho}^s].$$

Since $B[x^s ; \rho^s]$ and $B[x^{sp_j} ; \rho^{sp_j}]$ are H-separable extension over B, it follows from [9, Proposition 2.2] that $T^{p_j} - x^{sp_j}$ is an H-separable polynomial in $B[x^{sp_j} ; \rho^{sp_j}][T ; \tilde{\rho}^s]$. We shall show that the center of $B[x^{sp_j} ; \rho^{sp_j}] = Z^{\rho^{sp_j}}$. In fact, the center of $B[x^{sp_j} ; \rho^{sp_j}] \supseteq Z^{\rho^{sp_j}}$ is clear and for any $y = \sum_{\nu=0}^{q-1} (x^{sp_j})^\nu d_\nu$ in the center of $B[x^{sp_j} ; \rho^{sp_j}]$, we have

$$(\rho^{sp_j})^\nu (b) d_\nu = d_\nu b \ (b \in B) \quad \text{and} \quad \rho^{sp_j}(d_\nu) = d_\nu \ (0 \leq \nu \leq q-1).$$

Since $Y^q - u$ is an H-separable polynomial in $B[Y ; \rho^t] = B[Y ; \rho^{sp_j}]$, it follows from [3, Lemma 1(1)] that $d_\nu = 0$ $(1 \leq \nu \leq q-1)$. Hence $y = d_0 \in Z^{\rho^{sp_j}}$. Since $T^{p_j} - x^{sp_j}$ is H-separable in $B[x^{sp_j} ; \rho^{sp_j}][T ; \tilde{\rho}^s]$ and p_j is a prime number, $Z^{\rho^{sp_j}} / Z^{\rho^s}$ is a $(\rho^s | Z^{\rho^{sp_j}})$-Galois extension of order p_j by [4, Theorem 2]. Thus the assertion follows from Lemma 2.

In the proof of [4, Theorem 4] we have proved the following: Let $f = X^{p^e} - u$ be a separable polynomial in $B[X; \rho]$. If p is a prime number, and p is contained in the Jacobson radical $J(B)$ of B, then Z/Z^{ρ} is a $(\rho|Z)$-Galois extension, and the group $(\rho|Z)$ is of order p. We shall generalize this result as follows:

Theorem 3. *Let $f = X^m - u$ be in $B[X; \rho]$ with $fB[X; \rho] = B[X; \rho]f$, and $m = \ell p^e$, $(\ell, p) = 1$. Assume that p is a prime number, and p is contained in the Jacobson radical $J(B)$ of B.*

(1) *If f is a separable polynomial in $B[X; \rho]$, then Z/Z^{ρ^ℓ} is a $(\rho^\ell|Z)$-Galois extension, and the group $(\rho^\ell|Z)$ is of order p^e.*

(2) *If f is an H-separable polynomial in $B[X; \rho]$ and ℓ is a prime number, then Z/Z^{ρ} is a $(\rho|Z)$-Galois extension and the group $(\rho|Z)$ is of order m.*

Proof. (1) Since f is a separable polynomial in $B[X; \rho]$, it follows from [6, Theorem 3.1] that there exists an element $c \in Z$ such that

$$c + \rho(c) + \rho^2(c) + \cdots \rho^{m-1}(c) = 1.$$

We put here

$$d = c + \rho(c) + \cdots + \rho^{\ell-1}(c).$$

Then we have

$$d + \rho^\ell(d) + (\rho^\ell)^2(d) + \cdots + (\rho^\ell)^{p^e-1}(d) = 1.$$

We consider the polynomial $g = Y^{p^e} - u \in B[Y; \rho^\ell]$. Then g is a separable polynomial in $B[Y; \rho^\ell]$ by [6, Theorem 3.1] again. Since $p \in J(B)$, it follows from the proof of [4, Theorem 4] that Z/Z^{ρ^ℓ} is a $(\rho^\ell|Z)$-Galois extension and the group $(\rho^\ell|Z)$ is of order p^e.

(2) We have

$$B[x; \rho] \supset B[x^\ell; \rho^\ell] \cong B[Y; \rho^\ell]/(Y^{p^e} - u)B[Y; \rho^\ell] \supset B.$$

As was shown in (1), $Y^{p^e} - u$ is an H-separable polynomial in $B[Y; \rho^\ell]$. Since $B[x; \rho]$ is H-separable over B, it follows from [9, Proposition 2.2] that $B[x; \rho]$ is H-separable over $B[x^\ell; \rho^\ell]$. Naturally, we can extend ρ to the automorphism $\tilde{\rho}$ of $B[x^\ell; \rho^\ell]$. Consider the skew polynomial ring $B[x^\ell; \rho^\ell][T; \tilde{\rho}]$, where $aT = T\tilde{\rho}(a)$ $(a \in B[x^\ell; \rho^\ell])$. Since

$$B[x; \rho] \cong B[x^\ell; \rho^\ell][T; \tilde{\rho}]/(T^\ell - x^\ell)B[x^\ell; \rho^\ell][T; \tilde{\rho}],$$

$T^{\ell}-x^{\ell}$ is an H-separable polynomial in $B[x^{\ell};\ \rho^{\ell}][T;\ \tilde{\rho}]$. We shall show that $V_{B[x^{\ell};\rho^{\ell}]}(B[x^{\ell};\ \rho^{\ell}])=Z^{\rho^{\ell}}$. $V_{B[x^{\ell};\rho^{\ell}]}(B[x^{\ell};\ \rho^{\ell}])\supseteq Z^{\rho^{\ell}}$ is clear. On the other hand, for any $y=\sum_{\nu=0}^{p^e-1}(x^{\ell})^{\nu}a_{\nu}\in V_{B[x^{\ell};\rho^{\ell}]}(B[x^{\ell};\ \rho^{\ell}])$, we obtain

$$(\rho^{\ell})^{\nu}(b)a_{\nu}=a_{\nu}b\ (b\in B)\quad\text{and}\quad\rho^{\ell}(a_{\nu})=a_{\nu}\ (0\leq\nu\leq p^{e}-1).$$

Since $Y^{p^e}-u$ is an H-separable polynomial in $B[Y;\ \rho^{\ell}]$, it follows from [3, Lemma 1(1)] that $a_{\nu}=0\ (1\leq\nu\leq p^{e}-1)$. Hence $y=a_0\in Z^{\rho^{\ell}}$, and so $V_{B[x^{\ell};\rho^{\ell}]}(B[x^{\ell};\ \rho^{\ell}])=Z^{\rho^{\ell}}$. Since ℓ is a prime number, it follows from [4, Theorem 2] that $Z^{\rho^{\ell}}/Z^{\rho}$ is a $(\rho|Z^{\rho^{\ell}})$-Galois extension, and the group $(\rho|Z^{\rho^{\ell}})$ is of order ℓ. By (1), $Z/Z^{\rho^{\ell}}$ is a $(\rho^{\ell}|Z)$-Galois extension, and the group $(\rho^{\ell}|Z)$ is of order p^e. Then the assertion follows from Lemma 2.

Combining Theorem 3 and [2, Proposition 1.4] we have the following which is a generalization of [4, Theorem 4].

Corollary 4. *Let $f=X^m-u$ be in $B[X;\ \rho]$ with $fB[X;\ \rho]=B[X;\ \rho]f$, and $m=\ell p^e$, $(\ell,p)=1$. Assume that p is a prime number, and p is contained in the Jacobson radical $J(B)$ of B. If f is a separable polynomial in $B[X;\ \rho]$, then $g=Y^{p^e}-u$ is an H-separable polynomial in $B[Y;\ \rho^{\ell}]$.*

The following is a shapening of [4, Theorem 4], which corresponds to the results of Nagahara [7, Theorems 1 and 2].

Corollary 5. *Let $f=X^m-u$ be in $B[X;\ \rho]$ with $fB[X;\ \rho]=B[X;\ \rho]f$, and $m=\ell p^e$, $(\ell,p)=1$. Assume that p is a prime number, and p is contained in the Jacobson radical $J(B)$ of B. Then the following are equivalent:*

(a) *u is invertible in B^{ρ}, and Z/Z^{ρ} is a G-Galois extension, where G is the group generated by $\rho|Z$ of order m.*

(b) *$B[x^n;\ \rho^n]$ is an H-separable extension over B for every divisor n of m.*

(c) *$B[x;\ \rho]$ is a separable extension over B, $B[x;\ \rho]$ is an H-separable extension over $B[x^{\ell};\ \rho^{\ell}]$ and $B[x^r;\ \rho^r]$ is an H-separable extension over B for every divisor r $(1<r<\ell)$ of ℓ.*

(d) *$B[x;\ \rho]$ is a separable extension over B and $B[x^r;\ \rho^r]$ is an H-separable extension over $B[x^{\ell};\ \rho^{\ell}]$ for every divisor r $(1\leq r\leq\ell)$ of ℓ.*

Proof. (a) $\Longleftrightarrow$ (b) was shown in Theorem 1.

(b) $\Longrightarrow$ (c). Since both $B[x;\ \rho]$ and $B[x^{\ell};\ \rho^{\ell}]$ are H-separable extension over B, it follows from [9, Proposition 2.2] that $B[x;\ \rho]$ is an H-separable extension over $B[x^{\ell};\ \rho^{\ell}]$.

(c) $\Longrightarrow$ (d). Since f is a separable polynomial in $B[X; \rho]$, as was shown in the proof of Theorem 3(1), $B[x^\ell; \rho^\ell]$ is an H-separable extension over B. Hence by [9, Proposition 2.2], $B[x^r; \rho^r]$ is an H-separable extension over $B[x^\ell; \rho^\ell]$ $(1 \leq r \leq \ell)$.

(d) $\Longrightarrow$ (a). It follows from Theorem 1, Theorem 3(1) and careful reading of the proof of Theorem 3(2).

Acknowledgement. This work was done while the first author were staying at the Mathematics Department of Bradley University in spring 1992. He expresses his gratitude to the Mathematics Department for their hospitality.

REFERENCES

[1] S. U. CHASE, D. K. HARRISON, and A. ROSENBERG: Galois theory and Galois cohomology of commutative ring, Mem. Amer. Math. Soc. **52** (1965), 15—33.

[2] S. IKEHATA: Azumaya algebras and skew polynomial rings, Math. J. Okayama Univ. **23** (1981), 19—32.

[3] S. IKEHATA: Azumaya algebras and skew polynomial rings. II, Math. J. Okayama Univ. **26** (1984), 49—57.

[4] S. IKEHATA: On H-separable polynomials of prime degree, Math. J. Okayama Univ. **33** (1991), 21—26.

[5] S. IKEHATA and G. SZETO: On skew polynomial rings and Galois extensions, to appear.

[6] Y. MIYASHITA: On a skew polynomial ring, J. Math. Soc. Japan **31** (1979), 317—330.

[7] T. NAGAHARA: Some H-separable polynomials of degree 2, Math. J. Okayama Univ. **26** (1984), 87—90.

[8] H. OKAMOTO and S. IKEHATA: On H-separable polynomials of degree 2, Math. J. Okayama Univ. **32** (1990), 53—59.

[9] K. SUGANO: On centralizers in separable extensions, Osaka J. Math. **7** (1970), 29—40.

S. IKEHATA
DEPARTMENT OF MATHEMATICS
COLLEGE OF LIBERAL ARTS AND SCIENCES
OKAYAMA UNIVERSITY
TUSHIMA, OKAYAMA 700, JAPAN

G. SZETO
DEPARTMENT OF MATHEMATICS
BRADLEY UNIVERSITY
PEORIA, ILLINOIS 61625 U.S.A.

(*Received April 21, 1992*)

